Journal of Digital Convergence
Vol. 19. No. 4, pp. 133-139, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.4.133

블록체인을 이용한 모바일 DRM 기반 개선된 인증 메커니즘 설계 및 구현

전진오, 서병민*
성결대학교 파이데이아학부 교수

Design and implementation of improved authentication mechanism base on mobile DRM using blockchain

Jinl-Oh Jeon[1], Byeong-Min Seo*
Professor, Division of Paideia College, Sungkyul University

요 약 네트워크 기술의 비약적인 발전으로 모바일 디지털 콘텐츠 분야에서도 콘텐츠 보안 기술에 관한 연구가 활발히 이루어지고 있다. 그동안 콘텐츠 보호는 불법 복제 방지, 인증 그리고 인증서 발급/관리 등에 한정되었지만, 여전히 비밀정보 공개나 인증의 측면에서 많은 취약점이 존재한다. 본 연구는 휴대전화 번호 또는 단말기 번호를 통한 콘텐츠 다운로드 권한의 이중 관리를 기반으로 콘텐츠에 대한 비밀정보를 강화하고자 한다. 또한 3단계 사용자 인증 프로세스를 바탕으로 디지털 콘텐츠가 안전하게 배포되도록 강인한 모바일 DRM(Digital Right Management) 시스템을 구축하여 재전송 공격을 방지하고자 한다. 그리고 불법 복제 차단 및 저작권 보호를 위하여 사용자 인증을 기반으로 1차/2차 프로세스 과정에서 블록체인 기반 콘텐츠 보안 강화에 대해 연구하였다. 또한 정상적인 사용자가 제3자에게 본인 소유의 콘텐츠를 재분배하여 비정상적으로 콘텐츠를 사용할 때에도 이를 위해 3단계에 걸친 최종적인 권한 발급을 통해 Client 인증 과정을 더욱 향상시켰다.

주제어 : 블록체인, 모바일 DRM, 모바일 인터넷, 콘텐츠 유통, 콘텐츠 보안

Abstract Due to the rapid progress in network technology, many research on content security technologies is also being conducted in the mobile digital content sector. In the meantime, content protection has been immersed in preventing illegal copying, certifying, and issuance/management certificates, but still have many vulnerabilities in managing or authenticating confidential information. This study aims to strengthen confidential information about content based on dual management of content download rights through mobile phone numbers or device numbers. It also protect replay-attack by building a secure mobile DRM system where digital content is safely distributed based on a three-stage user authentication process. In addition, blockchain-based content security enhancements were studied during the primary/secondary process for user authentication for the prevention of piracy and copyright protection. In addition, the client authentication process was further improved through three final stages of authorization in the use of illegal content, considering that legitimate users redistributed their content to third-party.

Key Words : Blockchain, Mobile DRM, Mobile Internet, Content Distribution, Content Security

*Corresponding Author : Byeong-Min Seo(lightsalt@sungkyul.ac.kr)
Received January 11, 2021 Revised February 3, 2021
Accepted April 20, 2021 Published April 28, 2021

1. 서론

급속한 디지털 네트워크 환경의 발전과 mobile 기기의 일반화로 디지털 콘텐츠의 수요가 급증하고 있다. 그러나 디지털 콘텐츠는 대부분 mobile 인터넷으로 다운로드가 이루어지므로 콘텐츠 보안 관리가 미흡하다. 이에 대한 해결책으로 DRM(Digital Rights Management)이 등장하게 되었다[1, 2].

초기 DRM은 유선 환경에서 제공되어 오다가 현재는 가장 보편적인 mobile 인터넷 환경으로 자리하고 있다. 따라서 더욱 안전한 형태의 콘텐츠 보호를 위한 mobile DRM 연구가 요구되고 있다.

디지털 콘텐츠의 보안 요소로 주요 시퀀스 항의 비선형성을 높이고 상관 공격에 대비하는 알고리즘과[5], 퍼즐화 기술과 비밀번호 생성 기술을 사용하여 안전하게 암호화하는 방안이 연구되었다[6]. 그럼에도 불구하고 제안된 알고리즘은 mobile Phone과 개인 이동형 단말기와 같은 무선 환경에 직접적인 응용이 불편하다.

현재 모바일 DRM은 콘텐츠 보호를 위한 OMA DRM의 상용화가 이루어지지 않고 있으며 오히려 MPEGLA 등의 라이선싱 문제로 정체 상태에 있다. 다만 Apple을 위시한 솔루션 업체들이 One and Only One DRM 쪽으로 위치를 강화하고 있다. 모바일 환경에서의 주된 연구 과제는 식별자의 경량화, 호환성, 식별자 추출 및 정합의 성능향상이다.

기존의 Hash Function 등을 적용한 인증 방법은 사용자의 식별자가 쉽게 알려지는 단점과 메타데이터에 난수 정보를 추가로 삽입해야 하는 문제점이 있다. 때문에 블록체인을 이용하여 보다 강도 높은 암호화와 인증 및 분배 정책이 필요하다.

본 논문에서는 향상된 사용자 인증을 이용하여 mobile 환경에서 DRM 콘텐츠를 안전하게 배포하고 보호하는 유무선 디지털 콘텐츠 보안 시스템을 설계하고 구현한다. 제안된 시스템은 블록체인(Blockchain)을 적용하여 디지털 콘텐츠를 관리하고, mobile phone numbers, PDA 시리얼 번호 등의 정보를 검증하여 콘텐츠의 다운로드가 가능하도록 한다. 또한 권한을 분리함으로써 3단계에 걸쳐 사용자 인증이 이루어지도록 한다. 이 과정을 통해 DRM 콘텐츠가 보호되고 보다 안전하게 관리되는 DRM 시스템을 구현한다.

2. DRM과 mobile 인터넷 서비스

DRM이란 디지털 콘텐츠의 불법 사용을 차단하여 제작자의 권리를 보호하는 기법으로 여러 단계의 관계자들이 밀접적으로 연관되어 거래 및 비용 지불에 따라 다양하게 수익을 창출하고 있다.

다음의 Fig. 1.은 DRM 시스템에서 콘텐츠와 저작권에 대한 배포 흐름을 보여주고 있다[3].

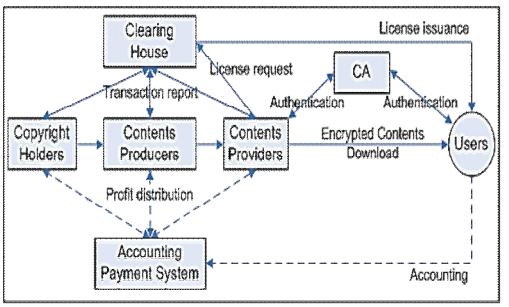

Fig. 1. Flow chart of content distribution in DRM system

mobile 네트워크에 적용되는 프로토콜은 유선 네트워크 환경의 HTML, XML, HTTPS 등을 기본으로 속도 향상을 위해 소형화하여 mobile 환경에서도 안정성 있게 사용할 수 있도록 하고 있다. 현재 대표적인 mobile 네트워크 프로토콜은 WAP 기반의 WAP과 HTTPS 기반의 ME 그리고 i-mode 등을 사용하고 있다[4].

그중에 WAP 기반의 WAP은 mobile 단말기에서 네트워크의 Access point에 연결하는 프로토콜 규약이다. 1차 유선 네트워크와 2차 무선 네트워크를 상호 연결하는 WAP 게이트웨이는 WML 콘텐츠를 부호화/복호화하고 종류가 다른 프로토콜을 서로 호환 가능하도록 해주며 또한 HTML 코드를 WML 코드로 바꾸어 준다.

그러나 네트워크 망을 통해 다운로드한 디지털 콘텐츠는 항상 보안의 취약점이 내재되어 있어 디지털 콘텐츠 제작자의 보호 측면에서 강화된 라이선싱 개념의 보안 메커니즘이 절대적이다. 현재의 보안 메커니즘은 디지털 콘텐츠 구매자의 ID를 콘텐츠와 함께 암호화하고 단일 분배 기능에 의해 콘텐츠의 정보, 권한, 인증 관련 등을 쉽게 적용할 수 있어 폭넓게 응용되고 있다.

이때 사용되는 기술은 디지털 콘텐츠에 공개키와 암호키 및 비밀키 그리고 암호 해독키를 단계적으로 적용하여 제작자의 소유권을 보장하고 있다. 그럼에도 이 방법은 복제 및 보안상의 한계점이 노출되고 있는 바 공용 및 내부 네트워크로부터 보다 안전한 암호화 데이터 스트림 전용 송수신 모듈의 적용과 이중 분배에 따른 안전성이

필요하다.

3. mobile DRM 구현을 위한 시스템 설계

3.1 mobile DRM 시스템의 기본 구성도

다음의 Fig. 2.는 WAP을 위한 공개키 기반구조(PKI) 모델을 이용하는 시스템 구성도를 나타낸다[4].

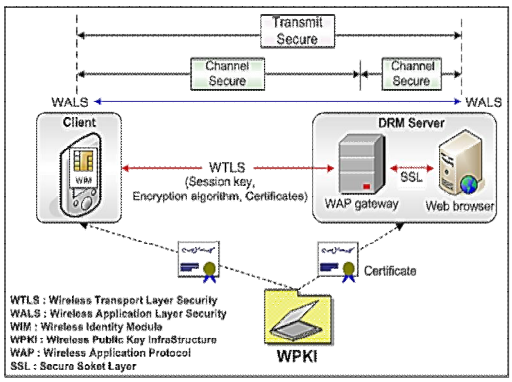

Fig. 2. System configuration diagram using WAP PKI

Client와 DRM Server가 서로 무선 네트워크 통신 규약을 통해 연결할 경우, 먼저 해당 프로토콜의 handshake 과정을 통해 콘텐츠 보안에 사용되는 자체 정보와 메타데이터 정보를 저장하고 이를 관리한다. 이 과정에서 생성된 프로토콜 세션 정보는 콘텐츠 보안 요소로 다른 계층의 record 프로토콜에 전달된다. 이때 이루어지는 보안 서비스는 사용자와 WAP Gateway까지 무선 프로토콜인 WTLS 사용하여 채널을 보호한다. WAP Gateway에서 웹브라우저까지의 보안 적용은 SSL 프로토콜을 사용한다.

3.2 시스템의 구조 설계

다음의 Fig. 4.은 본 논문에서 제안하는 mobile DRM 시스템의 구조를 나타낸다.

시스템 내부는 DRM Server와 Client로 분리된다. 콘텐츠 제작자가 등록한 디지털 콘텐츠를 암호화하는 Packager, 데이터의 저장과 암호화 그리고 Right를 발급해 주는 Rights Issuer, 또한 콘텐츠를 Server에서 다운로드하고, WAP Push Message를 이용하여 Rights Issuer에게서 콘텐츠의 권한을 전달받는 Client로 구성되어 있다.

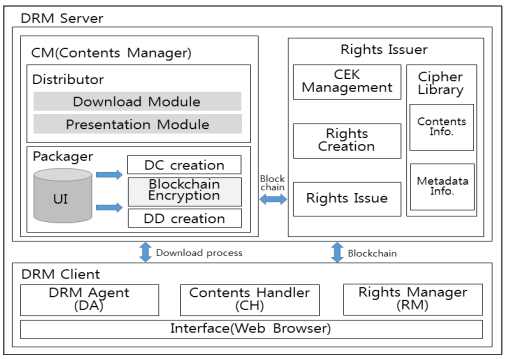

Fig. 3. mobile DRM system structure

제안한 시스템은 512비트의 공개키 블록체인 기반으로 설계되었다. 여기서 사용되는 공개키는 256비트씩 2개의 구조로 만들어진다. 512비트에 type을 구분하여 여기에 접두부 8비트가 더해져 520비트, 즉 65바이트가 1개의 공개키이다. Cilent는 난수발생기로 256비트의 비밀키를 생성하고 타원곡선암호방식으로 최종 512비트의 공개키를 생성한다[10, 11, 14]. 사용자가 콘텐츠를 요청하면 Download 모듈은 RI에게 해당 콘텐츠에 대한 사용 권한을 요청하게 되는데 이때 RI는 사용자에게 콘텐츠에 관련된 허가사항, 제한사항 및 콘텐츠 암호화 키가 포함된 객체의 비밀 정보를 사용 권한 REK(Right Encryption Key)로 암호화하여 발행해 준다.

또한 본 시스템은 모바일 DRM 시스템에서 문제없이 수행될 수 있도록 블록체인 암호화 방식을 적용하여 모든 모바일 단말기의 처리 성능을 극대화하는 방법으로 설계 및 구현되었다.

3.2.1 mobile DRM의 DRM Server

본 시스템의 DRM Server는 기능별로 크게 Contents Manager(CM)와 Rights Issuer(RI)로 구성된다.

CM은 Packager로 구성되어 있으며, 콘텐츠 정보와 DRM 콘텐츠를 리스트화하여 저장하고 있다. Distributor와 디지털 콘텐츠 제작자로부터 획득한 DRM 콘텐츠는 재생성된다. 모듈 구성은 Download 모듈과 Presentation 모듈로 구성되어 있다. Download 모듈은 Client가 콘텐츠를 요구할 때 해당 콘텐츠를 Client에게 전달해 주는 역할을 하며, Presentation 모듈은 DRM 콘텐츠 리스트와 기본 정보가 담긴 메타데이터를 브라우징한다. 콘텐츠 제작자가 제공한 DRM 콘텐츠를 암호화하고 콘텐츠의 기본 정보가 담긴 UI를 통하여 다운로드 가능한 DRM 콘텐츠로 Packaging 하며

DRM 콘텐츠의 메타데이터인 DD를 제공하는 것은 Packager 부분이다. 또한 콘텐츠를 암호화할 때 적용된 암호화 키는 권한 인증 객체에 종속되어 WAP Push 프로토콜을 이용하여 Client의 mobile 단말기로 전송된다.

Rights Issuer는 Packager로부터 콘텐츠를 획득하여 저장소에 저장, 관리하고 Cipher Library는 Right와 콘텐츠 암호화 키를 Client의 공개키를 이용하여 암호화한다.

3.2.2 mobile DRM Client(단말기)

DRM Client는 WAP을 통해 mobile 네트워크에 접속하는 이동형 네트워크 단말기를 말한다. Client 단말기는 DRM Server의 Contents Manager인 Distributor에 연결되어 DRM 콘텐츠를 다운로드한다. 이때 Client는 합법적인 권한이 발급된 경우에만 정상적으로 DRM 콘텐츠를 다운로드할 수 있다.

DRM Client의 구성은 DRM Agent(DA), Contents Handler(CH), Rights Manager(RM) 및 Interface(Web browser)로 이루어진다.

DRM Agent(DA)는 콘텐츠의 제공을 사용자의 권한에 준하여 제어하는 역할을 한다. 즉, CH(Contents Handler)에서 콘텐츠를 사용하겠다는 요청이 있게 되면 RM(Rights Manager)을 호출하여 Client의 권한을 승인하고, 그에 따른 권한이 적합한 경우에만 암호화된 콘텐츠를 복호화하여 실행할 수 있다.

CH는 응용 프로그램으로 DRM 콘텐츠를 사용자가 직접 사용할 수 있도록 해준다. Rights Manager는 비밀키와 공개키를 생성한 후 Rights를 암호화하고 이로부터 무선 응용 프로토콜의 Push Message가 확인되면 공개키를 전달한다. DRM 콘텐츠를 사용함에 있어 Right 정보를 점검하고 갱신한다. Interface는 mobile 인터넷에서 사용하는 웹브라우저를 이용한다.

3.3 mobile DRM 콘텐츠의 사용자 인증 절차

다음의 Fig. 4.는 mobile DRM 콘텐츠의 인증 절차를 나타낸다.

디지털 콘텐츠 제작자는 자신의 콘텐츠를 암호화한 후 CM에 등록하는데[12], 이때 블록체인을 이용한다. Client는 콘텐츠를 다운로드 받기 위해 ID, Password, 단말기 번호, mobile phone numbers 등을 입력하고 입력된 정보는 암호화된다. 이 과정에서 암호화된 정보는 차후 인증에 따른 권한을 이중으로 분리하기 위하여 RI에게 전송한다.

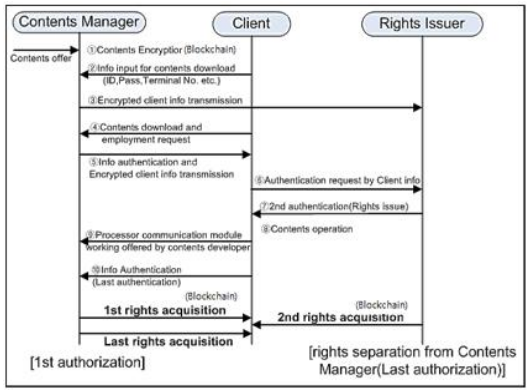

Fig. 4. mobile DRM content authorization process

Client는 CM에서 콘텐츠를 다운로드 받고 사용 요청을 한다. CM은 1차로 사용자가 입력한 정보를 비교하여 암호화 정보를 다시 사용자에게 전달한다. 사용자는 1차 권한을 발급받은 후 다시 RI에게 권한을 요청하고, 확인된 정보를 바탕으로 RI는 라이선스 권한을 발급한다. 이로써 CM에게서 다운로드한 콘텐츠의 사용 권한을 부여받고 콘텐츠를 실행하면 사용자와 통신을 하기 위해 콘텐츠 제작자가 제공한 프로세서 네트워크 모듈이 작동된다. CM은 한 번 더 메타데이터 등 사용자 정보를 이용해 콘텐츠의 최종 권한을 부여한다.

4. mobile DRM 인증 보안 시스템의 구현

본 논문에서 제안된 시스템은 Microsoft Windows Server 2019 환경에서 실험하였으며, 모바일 환경에서는 안드로이드 5.0 버전인 롤리팝과 Android Studio를 통해서 Server와 Client Device 간의 네트워크를 시험하였다. Packager는 .NET을 통해 설계하였으며[13], 콘텐츠 암호화 부분은 블록체인을 사용하였다. Packaging되는 콘텐츠를 다운로드 받고 실행할 Client는 Android Studio 환경의 Eclipse SDK에서 Android Studio AVD 에뮬레이터를 구성하여 가상으로 실험하였다.

4.1 제안한 시스템의 실행 과정

다음 Fig. 5.는 제안된 mobile DRM 시스템의 실행 과정을 보여준다. 1) 번부터 4) 번은 실행 순서를 나타낸다.

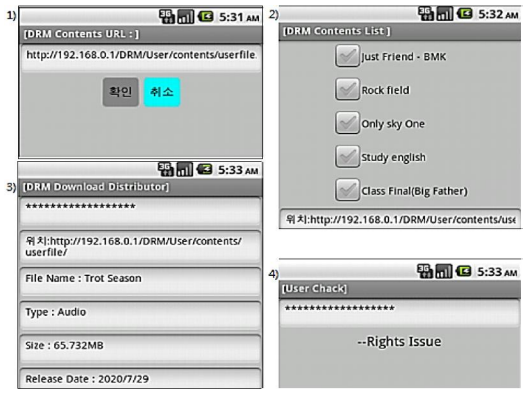

Fig. 5. Implementation process for obtaining 1st and 2nd authority

1) 번 단계는 디지털 콘텐츠 메타데이터와 DRM 콘텐츠를 보관하고 있는 DRM Server에 접속하는 과정이다. 이 과정은 단일 컴퓨터 환경에서 Server-Client 환경으로 구현했다. Distributor는 Client의 콘텐츠 다운로드 요청 시 해당 콘텐츠와 콘텐츠 리스트를 전송해 주는 역할을 한다.

2) 번 단계는 디지털 콘텐츠 제작자로부터 제공되는 Packaging 콘텐츠로 Distributor에게 전달되어 사용자가 디지털 콘텐츠를 요청할 때 Download 가능한 콘텐츠의 리스트를 보여준다. 사용자는 콘텐츠를 다운로드 받기 전에 자신의 ID, Password, 단말기 번호, mobile phone numbers, 권한 등의 정보를 입력하게 된다.

3) 번 단계는 디지털 콘텐츠 제작자가 자신의 콘텐츠를 블록체인을 이용하여 암호화한 후 CM에 등록한다. Client는 콘텐츠를 다운로드 받기 위해 기본적인 정보를 CM에 입력하고 그 내용은 암호화된다. 이 암호화 정보는 권한 분리를 위해 다시 RI에 전송된다.

4) 번 단계는 사용자가 콘텐츠를 요구할 때 사용자 정보 등을 검증하여 Client가 정당한 콘텐츠 사용자인지 확인한다. 정당한 사용자면 RI는 암호화 정보를 사용자에게 보내고, 사용 권한인 Right를 획득할 수 있다. 절차에 따라 사용자 인증이 끝나면 RI에게서 발급받은 Right로 인해 사용자는 다시 2차 권한을 획득한다.

4.2 사용자 인증 및 권한 발급 절차

4.2.1 최종 사용자 인증(1차)

콘텐츠 사용을 위한 1차 사용자 인증 단계에서는 먼저 제작자로부터 제공된 콘텐츠가 Distributor에게 전달되어 Packaging 된다. 최종 사용자가 Packaging 된 콘텐츠의 사용을 요청하고 이를 위해 사용자의 단말기 번호, mobile phone numbers, 권한 등의 정보를 입력하게 된다. CM은 콘텐츠와 사용자 정보를 Repackaging 하고 사용자가 실행을 위해 정보를 요구할 때 정보의 비교 검증을 한다. 이때 합법적인 사용자라면 입력 정보를 암호화하고, 이 과정에서 생성된 암호화 정보를 Server의 RI에게 전달한다. 이 절차를 통해 디지털 콘텐츠를 정상적으로 사용할 수 있도록 Right를 발급받게 된다.

4.2.2 최종 사용자 권한 인증(2차)

사용자의 1차 인증이 끝나면 RI에게서 발급받은 Right로 다시 2차 권한을 획득한다. 그러나 2차 권한을 획득한 콘텐츠도 다른 사용자에게 쉽게 전달될 수 있다. 때문에 1, 2차에서는 블록체인 기법을 이용하여 콘텐츠를 보호한다. Server의 관리 방법만으로는 차후에라도 보안상의 문제가 도출될 수 있으므로 콘텐츠 거래 시 모든 거래자들의 정보를 저장·관리하고 공유하여 불법 거래 및 사용이 이루어질 때 이를 대조해 제작자 콘텐츠의 위·변조 그리고 복제가 없도록 한다. 하지만 DRM 콘텐츠를 전달받은 다른 사용자는 콘텐츠를 사용하기 위해서 최종 권한을 다시 획득해야 한다.

4.2.3 최종 사용자 권한 발급(3차)

다음의 Fig. 6.은 사용자의 최종 권한 발급 그리고 프로세스 수행에 따른 콘텐츠의 실행 과정과 블록체인 관리 모듈을 보여준다.

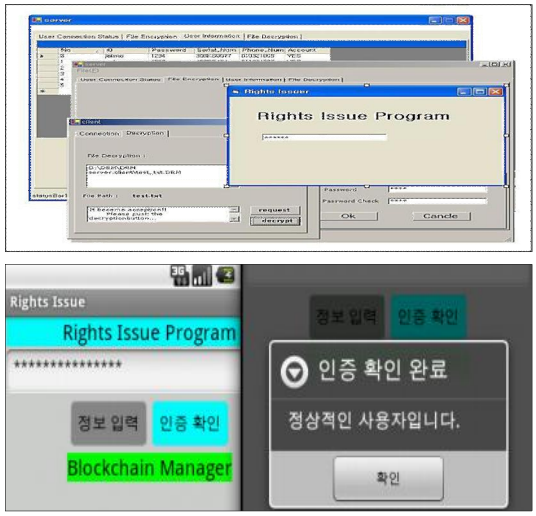

Fig. 6. Executed process of obtaining the final use rights

최종 권한을 RI에게서 획득하기 위해서는 먼저 1차 권한을 CM에게서 획득해야 한다. 이 과정에서 최종 권한을 RI에게서 획득했다 하더라도 다운로드한 콘텐츠를 실행하고자 할 때 다시 3차로 권한 인증을 획득해야 하므로 사실상 불법적인 콘텐츠 사용은 불가능하다. 네트워크 프로세서 모듈은 mobile 콘텐츠를 실행하고자 할 때 사용자의 메타데이터 정보와 비교하여 비용 결제를 하게 되고 이 절차를 통하여 정상적인 사용자에게만 확인 메시지를 전송해 준다. 확인이 완료된 사용자는 프로그램을 통하여 권한 인증을 받고 콘텐츠의 실행이 가능하다. 또한 콘텐츠 거래 과정에서 발생된 모든 정보를 저장소에 저장·관리한다.

콘텐츠 제작자가 제공한 네트워크 프로세서 모듈을 통해 최종 사용자의 인증 체계를 더욱 향상시키고 안전하게 사용할 수 있다. 결국, 사용자의 권한 발급과 인증 과정을 강화시키기 위해 이중으로 권한을 분리하고 3차에 걸쳐 단계별로 권한 승인이 이루어지도록 하였다.

4.2.4 기존 알고리즘과의 보안 성능 비교

다음의 Table 1.은 기존 알고리즘과의 보안 성능 비교를 보여준다.

Table 1. Security Performance Comparison with Existing Algorithms

Diagnosis	Correlation Attack	Puzzleization algorithm	Spectrum Water marking	Proposed mechanism
Mutual authentication	possible	possible	possible	possible
Transaction history analysis	Impossible	Impossible	shortage	possible
Location tracking	shortage	shortage	possible	possible
Copy protection	Unsafe	Unsafe	Unsafe	safety
Replay-attack	Unsafe	Unsafe	safety	safety
One and Only One DRM	Impossible	Impossible	possible	possible

상관 공격 알고리즘과 퍼즐화 알고리즘은 상호 인증은 가능하나 모바일에서의 적용은 불안전하다. 또한 스펙트럼 워터마킹은 거래 기록 분석, 복제 방지, One and Only One DRM에서 다소 미흡하다[15]. 제안한 메커니즘은 거래 기록 분석, 위치 트래킹, 복제 방지, Replay-attack 방지, One and Only One DRM이 모두 안전하게 이루어진다.

기존의 알고리즘이 Challenge-response 인증 절차로 사용될 때 Man-in-the-middle attack에 취약하며, 제3자로부터 공격에도 취약하다. 본 논문에서 제안한 시스템은 보안상 취약점을 해결하고 타 알고리즘에 비해 성능적으로 강인함이 입증되었다.

5. 결론

본 논문에서는 블록체인(Blockchain)을 이용한 모바일 DRM 기반 개선된 인증 메커니즘의 설계 및 구현에 대하여 기술하였다.

mobile DRM 콘텐츠 보호 방식 중에서 Separate Deliver 기법을 응용하여 콘텐츠를 암호화하고 휴대전화 번호 또는 PDA 시리얼 번호, 메타데이터 정보 등을 통하여 DRM 콘텐츠의 인증 권한을 향상시켰다. 그리고 Client 인증을 위하여 1차와 2차에서는 블록체인을 사용하여 콘텐츠를 보호했다. 특히 콘텐츠의 거래가 이루어질 때마다 거래자들의 정보를 저장, 관리하고 또 공유함으로써 불법적인 사용이 이루어질 때 이를 대조해 콘텐츠 자체의 위조와 변조 그리고 복제가 없도록 관리한다. 또한 합법적인 사용자가 본인의 콘텐츠를 제3의 사용자에게 재분배할 상황을 감안하여 복제에 따른 불법 콘텐츠가 유통되고 제작자 프로세서 네트워크 모듈을 피해 콘텐츠를 사용하고자 할 때 다시 3단계로 진행되는 사용자 인증을 통해 콘텐츠를 최종 사용하도록 권한을 강화함으로써 최종 사용자 권한 인증을 더욱 향상시켰다.

그럼에도 불구하고 mobile DRM 시스템은 콘텐츠 용량에 따른 요금 부과 및 취약한 보안 문제 그리고 블록체인의 보편적인 실용화가 남아 있으므로 차후 이 문제에 대한 관심 있는 연구가 필요하다.

REFERENCES

[1] C. N. Kim. (2003). *Next-generation Wireless Internet Services*. Electronic Times.

[2] G. S. Yoon. (2005). DRM Technology Status and Methods to Build Contents Distribution Infrastructure. *Journal of Korea Institute of Information Scientists and Engineers*.

[3] S. I. Jo et al. (2006). Proposal of an Encryption Algorithm Appropriate for Protection of Digital Contents. *Korea Information Processing Society*.

[4] G. H. Lee et al. (2006). A Study on Enhanced Protocol Security System for Protection of Multimedia Contents. *Korea Information Processing Society*.

[5] C. H. Seo. (2005). A Study of Security and Management

of Digital Education Contents based on DRM.

[6] C. Y. Gwak, Jo Myeonghw, So Uyeong. (2004). Design of DRM for Multimedia Contents Protection in Wireless Environment. *Korea Information Assurance Society*.

[7] I. J. Lee, K. K. Choi & D. Gorsich. (2010). Sensitivity analyses of FORM based and DRM based performance measure approach for reliability-based design optimization, *International Journal for Numerical Methods in Engineering, 82(1),* 26-46.

[8] Y. S. Jung, H. K. Cho & I. J. Lee. (2018). MPP-based approximated DRM using simplified bivariate approximation with linear regression, *Structural and multidisciplinary optimization : journal of ISSMO*

[9] F. Gartybgm & F. Ramme. (2000). watermarking of multimedia content for m-commerce application. *IEEE Communications Magazine 38(11)*. 78-84.

[10] Y. Hiroshi, (2017). *Information security and cryptography*, Korea : infinity books, p. 559-560

[11] Andreas M.Antonopoulos, (2017). *Mastering Bitcoin Second Edition*, California : O`Reilly, p. 57-66, p. 176-180, p. 196-200

[12] Li Xiaoqi, Jiang Peng, Chen Ting, Luo Xiapu, Wen Qiaoyan. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*.

[13] Joshua Duhl. (2001). *Digital Rights Management* : A Definition. IDC.

[14] B. Y. Jeon & J. H. Jeong. (2018). Digital Sharing Eonomy and Bockchain. *Trends and prospects*.

[15] Roman V. Glazkov, Oleg A. Guminskiy, Sergei V. Myshyanov, Nikita V. Babaev, Sergei A. Sokolov, (2020). Research and Implementation of Energy Dispersal Algorithm for DRM System, *Institute of Electrical and Electronics Engineers*

전 진 오(Jin-Oh Jeon) [정회원]

- 2001년 8월 : 국민대학교 전자계산학과(교육학석사)
- 2011년 2월 : 안양대학교 컴퓨터공학과(공학박사)
- 2017년 8월 ~ 현재 : 성결대학교 파이데이아학부 초빙교수
- 관심분야 : 인공지능, 빅데이터, 프로그래밍, 운영체제
- E-Mail : nobug5@naver.com

서 병 민(Byeong-Min Seo) [정회원]

- 2002년 2월 : 아주대학교 경영학과(경영학석사; e-Biz)
- 2014년 8월 : 한국외국어대학교 경영학과(경영학박사; MIS)
- 2016년 3월 ~ 현재 : 성결대학교 파이데이아학부 교수
- 관심분야 : ERP, e-Business, e-Learning, Blockchain
- E-Mail : lightsalt@sungkyul.ac.kr